STAFF SUMMARY SHEET

	TO	ACTION	SIGNATURE *(Surname)*, GRADE AND DATE		TO	ACTION	SIGNATURE *(Surname)*, GRADE AND DATE
1	Dpt Rsrch Director	sig	3 Mar 14 MARTIN C. CARLISLE, AD-24	6			
2	DFER	approve	SOLTI, AD-22, 13 MAR 14	7			
3	DFCS	action	DAVID J. CASWELL, MAJ	8			
4				9			
5				10			

SURNAME OF ACTION OFFICER AND GRADE Caswell, O-4	SYMBOL DFCS	PHONE 333-6803	TYPIST'S INITIALS djc	SUSPENSE DATE 20140314

SUBJECT Clearance for Material for Public Release USAFA-DF-PA- 181	DATE 20140312

SUMMARY

1. PURPOSE. To provide security and policy review on the document at Tab 1 prior to release to the public.

2. BACKGROUND.
Authors: Maj Michael Chiaramonte, Maj David Caswell, Col Gregory Schechtman

Title: The Case for an ABET Accredited Computer and Network Security Program

Circle one: Abstract Tech Report Journal Article Speech [✓ Paper] Presentation Poster

Thesis/Dissertation Book Other: ________________

Check all that apply (For Communications Purposes):

[] CRADA (Cooperative Research and Development Agreement) exists

[] Photo/ Video Opportunities [] STEM-outreach Related [] New Invention/ Discovery/ Patent

Description: Paper for 18th Colloquium for Information Systems Security Education

Release Information:

Previous Clearance information: (If applicable) N/A

Recommended Distribution Statement: Distribution A: approved for public release, distribution unlimited

3. DISCUSSION. The material is based on work to develop a computer and network security degree. The paper discusses the merits of having this type of degree ABET accredited.

4. RECOMMENDATION. Sign Coord block above indicating document is suitable for public release. Suitability is based solely on the document being unclassified, not jeopardizing DoD interest, and accurately protraying official policy.

DAVID J CASWELL, Maj, USAF
Assistant Professor

1 Tab: Tab 1) Paper for Approval

The Case for an ABET Accredited Computer and Network Security Program

Michael Chiaramonte, David Caswell, Gregory Schechtman
Department of Computer Science, United States Air Force Academy
2354 Fairchild Drive
USAF Academy, CO 80840 USA
michael.chiaramonte@usafa.edu
david.caswell@usafa.edu
gregory.schechtman@usafa.edu

Abstract – **Cyber security is a losing battle. Faced with the challenge of always being right, network defenders and secure systems developers are constantly being overwhelmed with attacks by nation states, criminal organizations and other hackers. This paper outlines the need for a formal program accreditation for cyber security academic programs as a means of meeting the nations need for personnel with deep understanding of cyber security spanning from hardware, software, and advanced technologies to risk mitigation, decision strategies, law, ethics and policy. This paper advocates for a multi-discipline ABET program accreditation to facilitate workforce hires, and skillset-job matching with a greater degree fidelity.**

Keywords – **Cyber, Security, Networks, Computer Science, Information Technology, Computer Engineering, Computing, Accreditation**

I. INTRODUCTION

Each year the number of cyber-attacks increases. These attacks have a profound impact on society including direct monetary losses, corporate and government privacy infringements, and lost consumer confidence. Today's users don't simply want immediate online access to bank accounts, stores, and social media. They implicitly demand secure access. This is evidenced by the outcry of the recent Target breach or increased scrutiny of time taken by Apple to push critical security patches.

These realities foster strong demand for highly educated computing specialists that understand the nuances of cyber security. Currently roughly 2% of all computing and mathematical graduates have earned a degree with some specialization in cyber security [1]. This is completely at odds with workforce demand for Cyber which needs at least 50,000 cyber specialists in the near future [1]. Additionally, these numbers do not reflect the need for cyber security understanding above the technical level. Managers, practitioners, legal departments, and senior leadership must understand how cyber security strategies can affect the bottom line. A recent PWC study showed that corporations with cyber security strategies in place fell victim to 50% fewer cyber security attacks than their competitors [2].

Similar to the past pushes for STEM education, the Federal Government has recognized the need for a holistic push for cyber education. The National Initiative for Cyber Education (NICE) lists as one of its major initiatives the expansion of cyber education. This initiative specifically highlights the limited focus of existing cyber training programs and the imperative to have a sound educational pipeline into the cyber security workforces of both the commercial and governmental sectors [4].

Despite the clear need for these professionals there is no official accreditation standard for undergraduate programs to follow. This lack of standardization obscures the comparative value of degree programs from students and leaves companies guessing as to what skills and knowledge the graduates may have acquired. This then encourages graduates to rely on certification programs to vouch for the students' credibility.

In this paper we will examine existing guidelines for computer and network security (CNS) programs. We then discuss different curricula developed by universities who offer CNS focused degrees. Having discussed the guidance and implementations, we then conclude with how an ABET accreditation would benefit this growing academic field.

As a note, we use the term computer and network security to refer to both information assurance and cyber education. While some will argue that these are independent topics, we view them as being so closely related that an educational program cannot teach one without understanding of the other.

II. EXISTING CURRICULA GUIDANCE

Currently there are no formally recognized academic program accrediting bodies that recognize CNS degree specializations. There are, however, a number of certifications that can be obtained by an institute of higher education to validate its programs. Two such certifications are awarded by the National Security Agency (NSA) and the Department of Homeland Security (DHS). The NSA/DHS currently certifies universities and colleges as either Centers for Academic Excellence (CAE) in Information Assurance (IA) or Cyber Operations. Table 1 lists a summary of the CAE criteria.

The CAE designations provide a good, and the primary, starting point for schools interested in designing a CNS program. They are, however, biased to support the needs of the NSA and DHS whereas not all programs are, nor should be, focused on developing students for the requirements of these government institutions. In addition, the large list of topics required by the CAE certification is not necessarily items that would or should be expected by students in an undergraduate program. This may make it difficult for undergraduate only institutions to achieve CAE status due to the lack of the course options available in graduate programs.

Another form of CNS related guidance is through the training organizations and their certification programs. With a lack of academic accreditations, employers often rely on these certifications to validate employee skilllevels. Such training certifications can be earned through organizations such as the SysAdmin Audit, Network Security institute (SANS) and the Information Security Institute (INFOSEC). These programs provide specialized training in a variety of CNS focus areas. SANS even has a regionally accredited graduate degree program. These certifications provide employers evidence of specialization in particular CNS topics however they do not provide the broad educational foundation that an undergraduate program is expected to imbue.

Table 1: Summary of criteria for NSA centers of excellence [6][7].

NSA-CAE Cyber Ops	NSA-CAE Info Assurance
Telecommunications	Database Management
Low-level Programming	Network Defense
Reverse Engineering	Networking
Operating System Theory and Virtualization	Operating Systems
Networking	Probability and Statistics
Cyber Offense/Defense	Programming
Vulnerabilities	Forensics
Legal Aspects	Software Security
Security Fundamentals	Security Management and Risk
Discrete Math	Mobile Technologies
SCADA	Security Planning and Design
Architecture and Embedded Systems	Analog and Digital Communications
Usable Security	Cryptography

III. COMPUTER AND NETWORK SECURITY CURRICULA

A. Who currently teaches undergraduate computer and network security

Despite the lack of formal accreditation many schools offer some form of a CNS degree. Table 2 lists several universities and their CNS style degree. Each of these programs provides undergraduate students an education focused on CNS topics. However, without the formal accrediting standards employers have little to rely on with regards to the skills being developed by the institution. This is the impetus behind NSA's development of the CAE programs.

Table 2: Example undergraduate degree programs with a cyber-security focus

School	Degree
University of Maryland and University Center	Computer Networks and Security
George Mason University	Cyber Security
New York University Polytechnic	Computer Science (cyber security focus)
United States Military Academy	Computer Science (information assurance focus)
United States Air Force Academy	Computer and Network Security

You will notice that two of the programs listed in Table 2 are tracks within an accredited Computer Science degree. While this is an option, we believe that more focus can be achieved by decoupling Computer Science from Cyber Security and treating each as a specialization within the world of computing.

B. The case for ABET Accreditation

Currently Computer Science, Computer Engineering, and Information Technology degrees all are accredited technical computing degrees. Each of these degrees have different foci that requires rigorous study to master. Computer Engineering focuses on hardware design and its interfacing with software. Computer Science develops algorithms for software and networking. Information Technology typically focuses on applied technology such as systems administration and network design. Each of these has some overlapping concepts and may include some security topics.

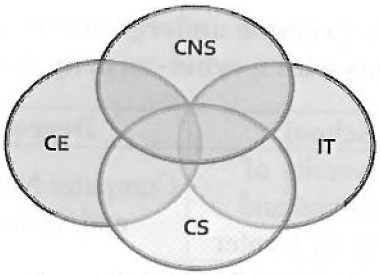

Figure 1: Relationship of major computing degree programs

Unfortunately, a computer and network security program needs to focus on a variety of topics that crosses all three programs as well as material that would not typically be included as primary criteria for any of these accepted programs. As an example, computer science and computer engineering both would work with assembly languages to understand how a program is working on the hardware. However, neither CS nor CpE typically has a need to study reverse engineering whereas this topic would be highly relevant to the Computer and Network Security graduate.

From a workforce perspective, having an accredited security focused degree provides employers and graduate schools knowledge of what to expect from students who earn a degree from these from accredited programs. This allows employers to hire from a variety of institutions with confidence that the incumbent has the required skills. Further, by having the academic approval that a Computer and Network Security accreditation provides, more employers may become more aware of the skill sets and thus become open to hiring in the field.

From the degree granting institution's perspective, having a computer and network security accreditation provides both guidance for the curricular depth and breadth as well as increases the credibility of the granted degree. While many programs could apply for the ABET General Computing Program this does not highlight the specialization of a Computer and Network Security professional.

Another key aspect of a CNS ABET program is to ensure that the programs do not cross the academic-training divide. An educational CNS degree must focus not on the tools but the theories that underpin the development, operations and management of secure systems. An example of training would be a Security + or CISSP course that prepares a person for a certification test. While the CISSP is a solid certification, it does not teach underlying fundamentals such a memory management or cellular network design strategies. As shown in Figure 2, it is the depth of understanding and the ability to apply these theoretical security fundamentals that distinguish CNS programs from training courses and other educational programs.

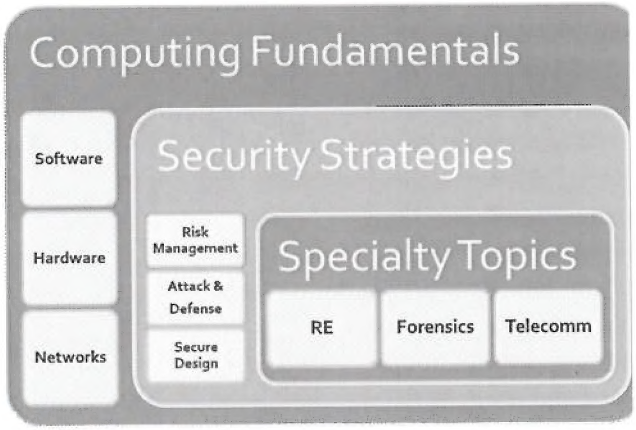

Figure 2: CNS builds on select topics from IT, CS and CpE programs to build security experts

IV. CONCLUSION

As computer security continues to grow as an accepted industry professions so to must academia grow to support the need. Without an ABET accredited CNS degree we leave students and employees in an uncertain realm as to what foundational knowledge is being developed in the different undergraduate programs. Employers are currently forced to rely on training certifications. While the NSA/DHS CAE provides useful guidance it is not tailored to support undergraduate programs. ABET has experience in developing for other key engineering technology degrees.

Developing cyber savvy professionals requires a focus on tailored topics from at least six disciplines. This unique characteristic must be accepted and integrated into collegiate accreditation programs to ensure that our professionals understand the business, political, legal, strategic, and technical implications of cyber. As Sandor Boyson, a research professor and cybersecurity expert, puts it: "There is an emerging need for cyber expertise that can be applied to business, policy and international issues. [9]" A CNS accreditation program would move the state of education closer to fulfilling this need.

As FBI director Muller put it, the "cyber threat will pose the number one threat to our country…Now we must position ourselves to best combat the cyber threat as it grows and morphs over the next 10 years" [3]. Developing rigorous criteria that validates the computer security credentials of undergraduate institutions is critical to the healthy development and sustainment of the professional workforce.

Disclaimer

The views expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the Department of the Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

[1] Fitzpatrick, Alexander. Online[May 2012]. "Cybersecurity experts needed to meet growing demand." *Washington Post*. Available at: http://www.washingtonpost.com/business/economy/cybersecurity-experts-needed-to-meet-growing-demand/2012/05/29/gJQAtev1yU_story.html.

[2] Loveland, Gary and Mark Lobel. Online[2012] "Cybersecurity: The new business priority," *PricewaterhouseCoopers View*, Issue 15. Available at: http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.jhtml.

[3] National Initiative for Cybersecurity Education. Online[October 2012].

"Cybersecurity Capability Maturity Model," White Paper. Available at: http://csrc.nist.gov/nice/documents/nice_capability_maturity_model_white_paper_082212_draft_nice_branded.pdf.

[4] National Initiative for Cybersecurity Education, *National Initiative For Cybersecurity Education (NICE)*, http://csrc.nist.gov/nice/aboutUs.htm.

[5] Defense Cyber Crime Center. 2014. *CDFAE*, www.dc3.mil/cdfae, retrieved March 2014.

[6] National Security Agency, 2013, *National Centers of Academic Excellence*, www.nsa.gov/ia/academic_outreach/nat_cae/, retrieved March 2014.

[7] National Security Agency, 2012, *National Centers of Academic Excellence – Cyber Operations*,www.nsa.gov/academia/nat_cae_cyber_ops/ , retrieved March 2014..

[8] National Security Agency, 2011, *Academic Requirements for Designation as a Center of Academic Excellence in Cyber Operations*, www.nsa.gov/academia/nat_cae_cyber_ops/nat_cae_co_requirements.shtml, retrieved March 2014.

[9] Russell, Joyce E. A. Online[October 27, 2013]. "Career Coach: There's plenty of jobs to be had in cybersecurity, but only if you are prepared." *Washington Post*. Available at: http://www.washingtonpost.com/business/capitalbusiness/career-coach-theres-plenty-of-jobs-to-be-had-in-cybersecurity-but-only-if-you-are-prepared/2013/10/25/57aef894-3c0f-11e3-b6a9-da62c264f40e_story.html.